DHMH E-Government Infrastructure Plan

Table of Contents

Introduction:

The purpose of an IT infrastructure is to provide a backbone of common services and support upon which users can build their applications. This infrastructure may not meet the needs of every user but we believe it meets the most common needs of most users.

This document describes the backbone that DHMH intends to build and the timeframe in which we expect it to be implemented. Thus, it is the blueprint for DHMH's future infrastructure services and support. It is also the implementation plan for DHMH's Architecture and Standards.

The requirements that this plan addresses are principally DHMH's current needs for network performance and capacity, continuous (7 X 24) operations and security. This plan will evolve as applications and usage grows. This plan reflects DHMH anticipated requirements over the next two fiscal years.

CAUTION: This plan describes what IRMA believes is required by DHMH and its internal Business Units and, therefore, what IRMA intends to implement and when. However, this plan is not funded. It is our intent to obtain funding from a variety of sources including DBM, DHMH and DHMH Agencies in the timeframe described but there is no assurance of success in obtaining funding. Any assistance you can provide -- being an advocate for the plan, financial support and/or other help -- will greatly assist us.

IRMA has demonstrated its ability to build, operate and manage the DHMH infrastructure. To meet today's needs, the infrastructure must be extended to address new requirements, most notably e-Government (e-Gov) and HIPAA (the Health Insurance Portability and Accountability Act). This plan is that next step.

What This Document Is:

The purpose of this document is to provide guidance to DHMH users (and other interested parties) about the strategic direction for IT infrastructure within DHMH and how best to use that strategic blueprint to your advantage. It accomplishes four objectives:

First, this document communicates the plan to affected parties. Users need to know what service and support resources they can count on and when. Management needs to know what resources are required to implement the plan and when. Finally, IRMA needs a blueprint for action. This document serves those purposes.

Secondly, this document describes the DHMH infrastructure plan. This plan is designed to provide a robust and secure network infrastructure, including network performance, capacity, high-availability and security for E-Gov applications and HIPAA over the next two years. The plan is consistent with the DHMH Architecture and Standards blueprint (described elsewhere. The principal capabilities that this plan addresses include:

1. Network performance and capacity
2. Continuous Operations (i.e., 7 X 24)
3. Security infrastructure
4. Remote access, including extending high-speed access to principal DHMH facilities (e.g., hospitals)
5. Physical space to support an Operations Center
6. Software Management Tools to manage the environment

This plan does not address requirements such as mainframe function and/or capacity, PC requirements and/or new user applications. These requirements are covered by individual Business Units within their IT Master Plan.

We anticipate a gradual buildup of services and support capabilities. In most cases, we anticipate a staged implementation, starting with basic functionality, followed by pilot applications, building to meet performance and capacity requirements, and evolving to full-function, continuous (7 X 24) operations.

Third, this document relates user plans and requirements to the functions this infrastructure plan addresses, i.e., why the functions are needed. As will become apparent, these capabilities are interdependent. They must be viewed as a

collection of components, all of which are required to meet the infrastructure goals. They cannot be partially implemented nor can they be partially funded.

Finally, this document is a request for help in developing a single DHMH infrastructure. That assistance may take many forms including advocacy for these requirements (both within DHMH and with other State Departments), financial assistance and, perhaps most importantly, communication and cooperation between IRMA and internal Business Units.

Who is Affected:

The e-Gov infrastructure described in this document primarily applies to DHMH users that are now or will develop e-Gov applications and/or are affected by HIPAA requirements. It is also important to other organizations that need to interconnect and/or interoperate with DHMH.

Within DHMH, the Business Units most affected due to near-term applications include Vital Records, Women, Infants and Children Program (WIC), Community Health Administration (CHA), Family Health Administration (FHA), Mental Hygiene Administration (MHA), Medicaid, Developmental Disabilities Administration (DDA), Board of Physicians Quality Assurance (BPQA), Office of Health Care Quality (OHCQ) and the Board of Nursing. In addition, there are numerous internal Business Units that are planning applications based on the availability of infrastructure services. Outside DHMH, many State agencies (including DBM, DNR, DHR, DOE, Public Safety and the Comptroller) as well as External Business Partners (including hospitals, medical professionals and pharmacies) and local Health Departments are or will be dependent upon delivery of services via the Internet. Finally, the citizens of Maryland are or will become dependent upon this infrastructure for DHMH services.

Perhaps most affected is DHMH itself. As DHMH increasingly delivers its services electronically, applications must be perceived to work, to perform well, to be continuously available and to be secure. DHMH's reputation and credibility are at stake. The best assurance of fulfilling these requirements is to control its own destiny with dedicated resources.

Why is this Document Important?

This document describes DHMH's strategic infrastructure plan. It details what components of infrastructure need to be rolled out and when and, therefore, what services and support users will be able to count on. If this plan is delayed, there are serious impacts that create the risk of failure for DHMH users in their e-Gov applications and HIPAA implementation.

DHMH's goal is to improve health care for the citizens of Maryland. To a large degree, its strategy to accomplish this is based on e-Gov applications and HIPAA. This infrastructure addresses the known needs of both.

e-Gov applications that depend upon this infrastructure and will be implemented during FY02 and FY03 include: Vital Records, WIC, CHA, FHA and MHA. These applications require consistently good response times, continuous availability and a high level of security to fulfill their mission and meet public expectations. Without these capabilities, theses Business Units will (necessarily) find commercial alternatives to fulfill their requirements.

HIPAA requires these services and support due to its mandated requirement for privacy (and, therefore, security) of medical data beginning in FY 03 and beyond. While HIPAA does not require use of the Internet (or other electronic means) of delivery, most organizations (including DHMH) are planning to use electronic delivery. As a result, security, data integrity, continuous operations and business resumption strategies are intimately tied to HIPAA implementation. Failure to protect the privacy of medical data can result in fines, loss of Federal funding and, perhaps most importantly, loss of credibility at the State and Federal levels.

Today, DHMH user needs have moved beyond the capabilities of the current infrastructure to support them. Agencies (including DDA, ADAA, BPQA, Medicaid and Board of Nursing) have already outsourced their e-Gov applications infrastructure to commercial vendors such as CSC and USi that can provide the infrastructure that DHMH lacks. While this may be a viable short-term solution, it results in 1) higher costs long-term and 2) the loss of interconnectivity and interoperability through the creation of non-standard and incompatible "islands of automation". These impacts will become worse over time. The practical effect is that DHMH is funding the construction of the commercial vendor's infrastructure.

As an example, five Business Units (Medicaid, DDA, MHA, BPQA and the Board of Nursing) have already outsourced their e-Gov infrastructure. Today, these Agencies are spending an estimated $20K per month for network services (includes Medicaid @ $12K per month and DDA @ $6K per month) with that amount expected to increase by 35 percent to 50 percent over the next six months. That cost will continue to escalate as transaction volumes grow and additional applications are deployed.

If this plan is not funded, users will continue to make their plans based on the non-availability of a DHMH infrastructure. They will necessarily either delay implementation of their applications or seek alternative short-term solutions (e.g., commercial vendors) to solve their needs. These solutions will invariably result in the loss of standardization and the erosion of the current infrastructure as users move away to alternative solutions. There will be fewer and fewer users sharing a fixed cost, which will, in turn, drive them away too. DHMH will devolve into "islands of automation" that cannot interconnect and/or interoperate. As that

occurs, Architecture and Standards will erode resulting in the loss of interconnectivity and interoperability. Thus, the decision to not build a DHMH infrastructure will have a profound impact on fulfilling DHMH's mission.

There are risks associated with this plan. 1) By far, the biggest risk is the lack of funding. Without that, DHMH cannot acquire the assets required to implement the plan. 2) This plan is dependent upon new technologies that require additional staff and new skills beyond current staffing needs. Without these people and skills, we may be able to implement the physical assets but they cannot be managed effectively. People and skills are required to succeed. 3) Finally, as with any new technology, there is a learning curve before the technology is fully understood, stabilizes and becomes a robust operating environment. We believe we have effectively planned for and can manage this risk through a staged rollout but, nevertheless, the risk is present. 4) There is no physical space (including reliable power) to house this additional technology or the staff to support it.

What Should Users Do?

This document is provided as guidance. It shows DHMH's strategic intent, i.e., the direction in which the DHMH "ship" will go. We expect that users will develop their e-Gov and HIPAA plans based upon this blueprint.

Because there are significant dependencies, we strongly recommend that you work closely with IRMA management to communicate and coordinate your plans as well as to understand the current status of the rollout of the infrastructure.

Perhaps the most important action that you can take is to clearly advocate the need for these network and security infrastructure requirements. Tell someone - your management, your business partners and you staff. If you agree with this plan, voice your support for a DHMH infrastructure as well.

Summary:

The purpose of an IT infrastructure is to provide a backbone of common services and support upon which users can build their applications. This infrastructure may not meet the needs of every user but we believe it meets the most common needs of most users.

This plan will result in the network performance and capacity, the highly reliable continuous operations and the security that DHMH needs for the future. We believe that the best way to achieve those goals is through an internal DHMH infrastructure.

If this plan is delayed -- most likely due to funding -- it will seriously impact user plans for E-Gov applications and HIPAA compliance.

Function by User

	Network Performance / Capacity	Continuous Operations	Function Security	Connectivity	Remote Access
Users					
Vital Records	Required	Required	Required	Required	Required
WIC	Required	Not Required	Required	Required	Required
CHA	Required	Required	Required	Required	Required
FHA	Required	Required	Required	Required	Required
MHA	Required	Required	Required	Required	Required
HIPAA	Required	N/A	Required	Required	Required
Outsourced					
Medicaid	Required	Required	Required	Required	Required
DDA	Required	Required	Required	Required	Required
Board of Nursing	Required	Required	Required	Required	Required
BPQA	Required	Required	Required	Required	Required
OHCQ	Required	Required	Required	Required	Required

Components by Function

	Component by Function			
	Network Performance / Capacity	Continuous Operations	Security	Connectivity	Remote Access
Component					
Remote Access					Yes
LDAP			Yes		Yes
Digital Certificate			Yes		
ISP	Yes	Yes			
Datacenter Facilities	Yes	Yes	Yes		
ATM	Yes				
T1 Lines				Yes	
VPN			Yes		Yes
Power Generation hookup		Yes			
Security Management Software			Yes		
Network Management	Yes		Yes		
Digital Encryption			Yes		
SSL			Yes		
ISP Redundancy	Yes	Yes			
Router		Yes			
DSU		Yes			
Distribution Switch		Yes			
Switch		Yes			
Firewall		Yes			
Local Distributors		Yes			
DNS		Yes			
Clustered Servers		Yes			
DHCP Servers		Yes			
Cache Servers		Yes			
UPS		Yes			
VPN Management Software			Yes		Yes
Firewall Management	Yes		Yes		
Novell 6.0	Yes				
Groupwise 6.0	Yes				
Tokens			Yes		
Smart Cards			Yes		
Radius Access Server					Yes
Smart Card Readers			Yes		
Bandwidth Upgrades	Yes				
Core Switch Upgrades	Yes	Yes			
Network Redundancy	Yes	Yes			
2nd (Hot) Site		Yes			

TIMELINE

1Q FY 02	**2Q FY 02**	**3Q FY 02**	**4Q FY 02**
Function	Remote Access Pilot	Digital Encryption Pilot	Token Operational
	LDAP Pilot	SSL Pilot	Smart Card Pilot
	Digital Certificate Pilot	Redundancy/Perf/Capacity	
	ISP Operational	ISP Redundancy	
	Datacenter Facilities		
Hardware/Software	ATM #1	ATM #2	Radius Access Server
	9 T1 Lines	Router (1)	Smart Card Readers
	VPN	DSU (1)	
	Power Generation hookup	Distribution Switch (2)	
		Switch (1)	
		Firewall (1)	
		Local Distributors (2)	
		DNS	
		Clustered Servers	
		DHCP Servers (2)	
		Cache Servers (4)	
		UPS	
Management Tools	Security Management Software	VPN Management Software	
	Network Management Software	Firewall Management	
		Novell 6.0	
		Groupwise 6.0	

1Q FY 03	2Q FY 03	3Q FY 03	4Q FY 03
Bandwidth Upgrade	Remote Access Operational	Digital Encryption Evaluation	Digital Encryption Operational
	LDAP Operational		2nd (Hot) Site
	Digital Certificate Operational		
	SSL Operational		
9 T1 Lines	Network Redundancy		
Core Switch Upgrades (2)	Core Switch Upgrades (2)	Core Switch Upgrades (2)	Core Switch Upgrades (2)